
Distributed Architecture

White Paper

Document ID: IC-135-TC009-1.1
Dated: 15th August 2008
Status: Released

This document describes two different approaches to saving data in an IP Video system. A **Centralised Architecture** uses a master database usually located in the central control room or head office. A **Distributed Architecture** spreads the data around the Security Management system generally keeping it close to where it is produced or needed. This document discusses the serious scalability problems which arise with a Centralised Architecture and how a Distributed Architecture gives a scalable solution leading to unlimited Security Management system sizes potentially spanning cities, countries and continents.



IndigoVision

Confidential Proprietary Information and Copyright Notice.

Copyright © 2008 IndigoVision Limited. All rights reserved.

Signatories

Chief Technical Officer.....

Program Manager

Contents

1. INTRODUCTION.....	4
2. IP VIDEO ARCHITECTURE	5
2.1 Scalability problems with a Centralised Architecture:	5
2.2 Scalability solutions with a Distributed Architecture:.....	6
3. EXAMPLE SMALL SECURITY MANAGEMENT SYSTEM	8
4. EXAMPLE MEDIUM SECURITY MANAGEMENT SYSTEM	9
5. EXAMPLE LARGE SECURITY MANAGEMENT SYSTEM	10

1. Introduction

This document describes two different approaches to storing data in an IP Video system. A **Centralised Architecture** uses a master database usually located in the central control room or head office. A **Distributed Architecture** spreads the data around the Security Management system generally keeping it close to where it is produced or needed.

The stored data in a Security Management system can be categorised into two types:

1. **Configuration** data such as site information specifying the design and make-up of the Security Management system. Examples of Configuration data includes lists of cameras, lists of users, user permissions, site structure and maps representing the layout of the system. After the initial installation and commissioning stages of a Security Management system, Configuration data is not routinely changed. It is however routinely read by operators e.g. when logging in to the system.
2. **Live** data such as CCTV video recordings and alarm data. Live data is accessed continuously during normal Security Management operations, either by devices recording the data or operators reviewing the data.

Configuration data is usually held in a database called the **Site Database**. This makes it easy for administrators to make and manage changes however it also creates a problem. When an administrator makes a change to the Site Database how do the users, distributed throughout the Security Management system, get the change?

The obvious and easy solution is to have the Site Database held centrally on a master database server and have all users access the master server over the network. This is called a Centralised Architecture.

Many systems use a Centralised Architecture for storing more than just Configuration Data. They may also use it for storing Live Data such as video recordings or alarm data.

This document discusses the serious scalability problems which arise with a Centralised Architecture and how a Distributed Architecture gives a scalable solution leading to unlimited Security Management system sizes potentially spanning cities, countries and continents.

2. IP Video Architecture

2.1 Scalability problems with a Centralised Architecture:

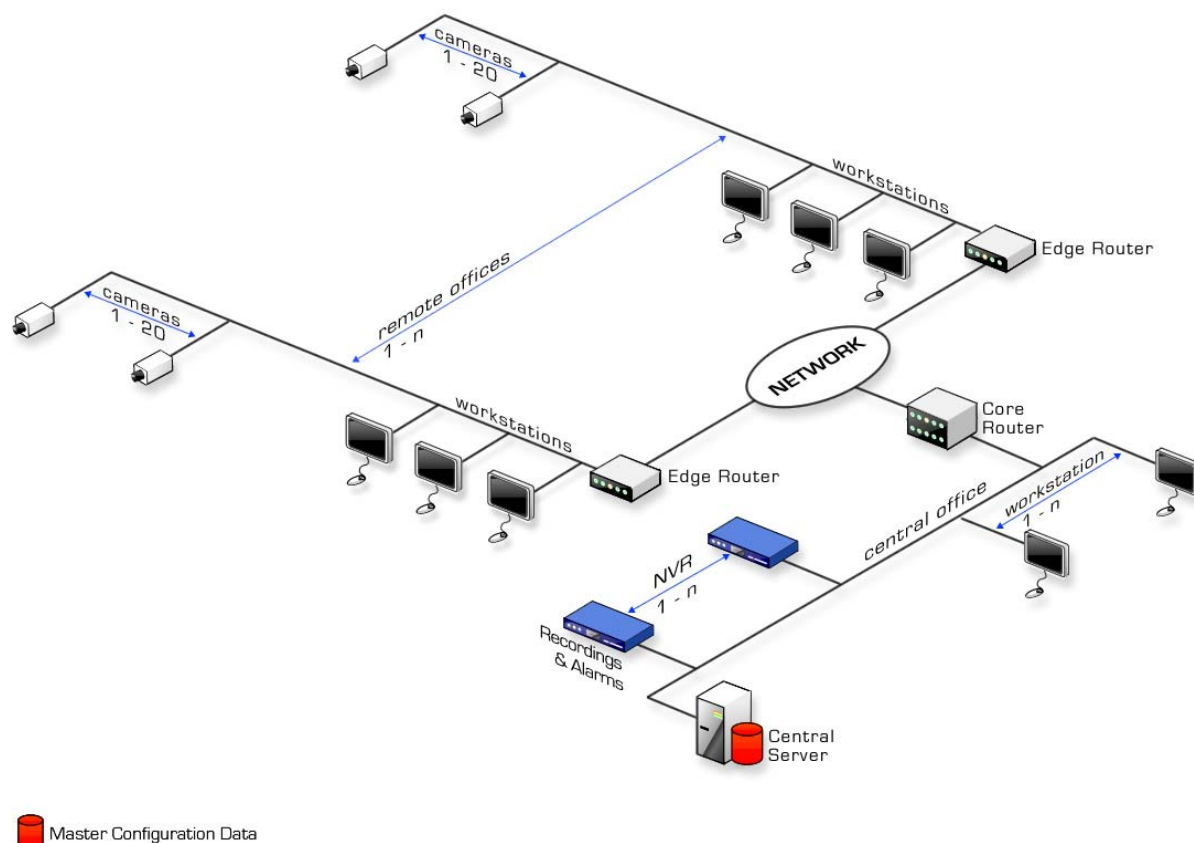


Figure 1 Typical Centralised Architecture

Figure 1 above shows a Security Management network consisting of one or more sites each with its own Local Area Network (LAN) connected to a Central Office. The Central Office is also where the Central File Server is located, hosting the Site Database. Also in the Central Office are Network Video Recorders (NVRs) for recording CCTV video and Alarm data.

Every camera and workstation in each remote office must regularly, and in some cases continuously, communicate with the Central Office in order to check for changes and updates in the Site Database, check for valid licensing or store recording and alarm data.

This causes four huge problems:

1. **Cost:** All users continuously communicate with the Central Office. On a LAN that means buying expensive high-end switches and on a WAN it means using up precious bandwidth.
2. **Reliability and Resilience:** What happens when the WAN or core LAN switch breaks? Remote users can be left stranded with no access to the live

and recorded video from cameras which are actually located locally to them on a working LAN.

3. **Single point of failure:** What happens if the server hosting the Site Database fails? All users of the system rely on access to the site database. For example to get login credentials verified or license permissions checked. If the Site Database server fails, the whole Security Management system goes down.
4. **Scalability:** As more cameras and users get added to each remote office and as more remote offices get added to the network, everything gets congested. The local LAN's get congested, the WAN links get congested and the Central Server gets congested coping with increasing levels of traffic checking for Site Database changes, valid licensing and storing recordings and alarms.

2.2 Scalability solutions with a Distributed Architecture:

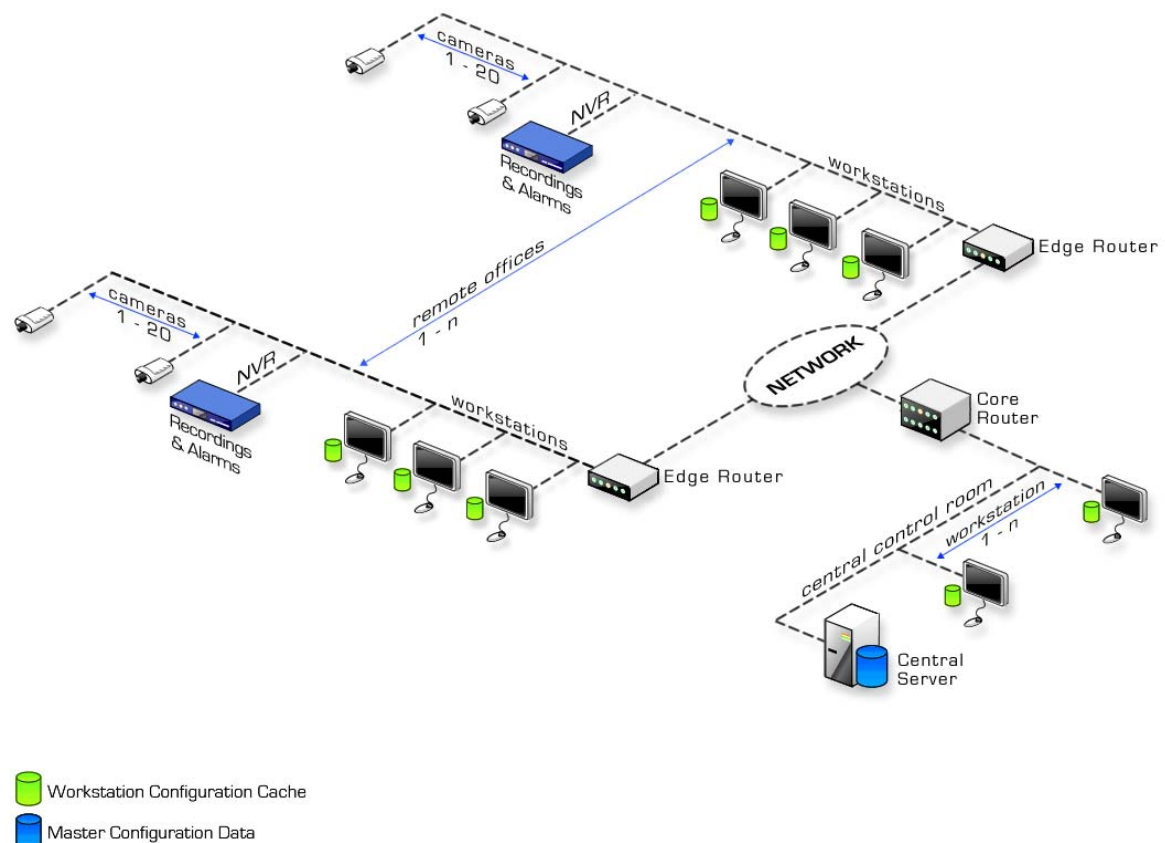


Figure 2 Distributed Architecture

The Distributed Architecture figure above shows how the same Security Management network can be constructed using distributed databases.

2.2.1.1 Distributing Configuration Data

To distribute configuration data, each remote workstation can keep a local cache of the Site Database. Configuration data does not change very frequently. This means the information can be synchronised between the Central Server and the remote workstations either according to a managed schedule or on-demand when a change happens.

In the event that the Central Server, a core LAN switch or the WAN fails, users at workstations can continue to work using their locally cached Site Database.

2.2.1.2 Distributing Licensing Data

Rather than holding license information centrally in the Central Server, individual components of the SECURITY MANAGEMENT system can hold their own licenses. For example, cameras can hold information in their on-board memory about allowed viewing and recording resolutions, or allowed frame rates. They can also hold information on which features are enabled such as advanced motion analytics features.

Such a model, where the sources of the valuable data (the cameras and recorders) contain their own licenses, means that the cameras and recorders never need to talk to the Central Server. Because the data sources have their own distributed licenses, this frees up the data viewing applications, running on each workstation, from requiring any license at all. An operator can't view video if the camera or recorder won't let him. This means none of the workstations need to check licensing conditions with the Central Server.

2.2.1.3 Distributing Live Data

Rather than continuously streaming recording and alarm data back from the remote sites to the central site across the WAN, it would be much better to keep the data locally on the LAN. One or more local Networked Video Recorders at each remote Site would reduce traffic across the WAN and allow users at the remote sites to access recordings and alarms even when the WAN is not available.

Of course the Central Office is often where alarm management happens across the whole Security Management system so users in the Central Office can still access the remote Networked Video Recorders in the event of an alarm or incident investigation. Usually when this happens they only need to playback or export certain portions of video from certain cameras and don't need to access the full 24x7 recordings that have been made of all cameras at the remote site.

2.2.1.4 Solving the problems of a Centralised Architecture

1. **Cost:** Precious WAN bandwidth is not used for continuous communication with all remote devices. Instead Configuration Data is distributed in a managed scheduled way. In the event of an operational incident, only the Live CCTV video data that is required need be moved across the WAN or extended LAN. The need to check license data across the network is removed entirely. Core network switches can be specified to cope with reduced network loads.
2. **Reliability and Resilience:** A critical source of failure in the Security Management network is the WAN. Money can be spent on increasing the reliability of the WAN connections but it is much more effective to distribute the data so that users still have a working Security Management system even if the WAN connections fail.

3. **Single Point of failure:** Another critical source of failure in the Security Management system are the data stores – either the Central Server hosting the Site Database or the recorders. Again, money can be spent on increasing the power and reliability of those machines but it is much more effective to distribute the data stores so that users still have a working Security Management system even if those components fail.
4. **Scalability:** With a distributed architecture, each remote office really can be treated as a template and simply duplicated as necessary. For even larger systems, there is no reason why multiple Central Servers can't be distributed and synchronised adding yet another layer of distribution and resilience.

3. Example Small Security Management System

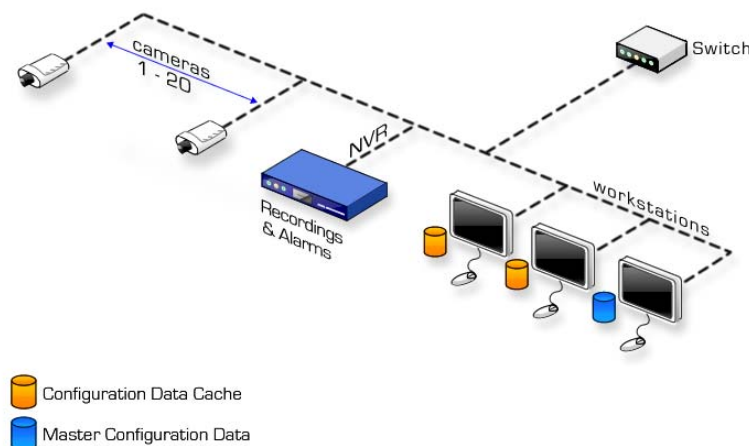


Figure 3 Small Distributed Security Management System

Even in a “small” Security Management system consisting of 20 cameras, 1 NVR recorder and 3 operator workstations, there are advantages to the distributed approach. One workstation can be chosen to host the “master” site database. This can then be shared using standard network file sharing options and the other workstations can point at this master copy. In addition they will keep local caches to cope with the event that the master workstation fails.

This allows the site administrator, who can be logged in to any of the workstations, to make changes to the master site configuration. The architecture automatically distributes the changes to the other workstations.

Using standard file sharing, updates are notified only when they happen so that each workstation can refresh its local cache as necessary.

4. Example Medium Security Management System

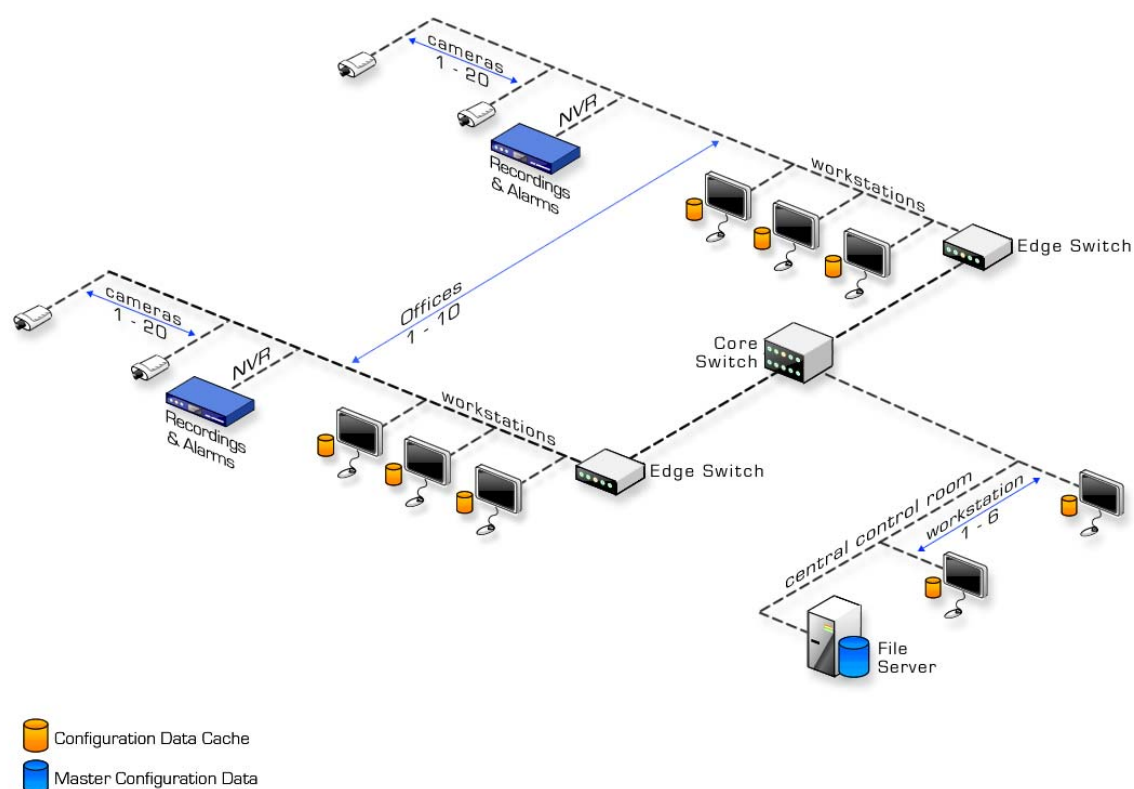


Figure 4 Medium Distributed Security Management System

A medium sized Security Management system might consist of up to 200 cameras spread across several distinct locations (floors on a building or buildings on a campus). Some operators may be located at each location but also there will typically be one central control room where several operators monitor the entire site.

With a distributed approach, the master configuration data will be held in a dedicated file server in the central office. Each workstation will use the file server as its primary source of configuration data but will also hold a local cache of the data.

Live data (recordings and alarm logs) will be distributed to each location by placing Network Video Recorders around the network. This keeps the majority of the live Security management data away from the central control room.

There are several advantages to this approach:

- Medium sized Security Management systems generally have a greater requirement for resilience. The file server can be stored securely and safely away from the operational control room. If the file server fails, workstations

still have local caches so there is no interruption to the Security Management system.

- By separating the **Static** configuration data from the **Live** Security Management data, the processing and disk space demands of the master site database is minimal meaning the “file server” can be entry level server. For example, a site database for a 200 camera system need contain no more than 100 Kbytes of data.
- Recording and alarm data need only be fed back to the central control room on demand (e.g. when investigating an incident). With a centralised architecture, all recording data would continuously be fed back from all cameras requiring more costly infrastructure

5. Example Large Security Management System

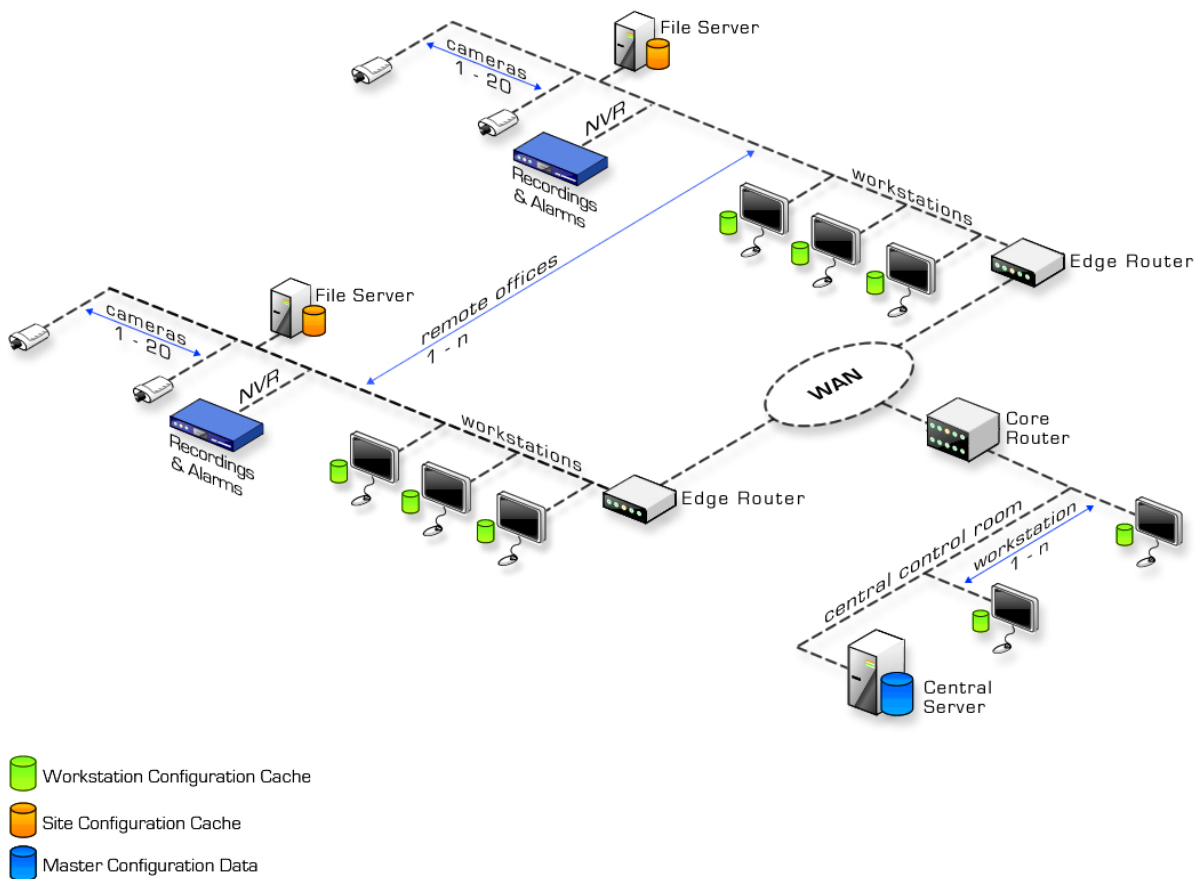


Figure 5 Large Distributed Security Management System

A large Security Management system will consist of thousands of cameras spread across many locations. Sometimes these locations will be geographically dispersed across cities, countries and even continents e.g. city surveillance, a large corporation, railway system or road system. Sometimes there may be one large location with a high density of cameras split into different groups of cameras e.g. casinos or airports.

Large systems will also usually have a central control room from where the whole system can be monitored. Some systems will have several such central control rooms. The entire network is linked by a Wide Area Network (WAN), which may use leased lines, wireless connections, DSL connections, satellite links and even the public Internet.

Under a distributed architecture, each location or group of cameras has a local file server and all workstations at that location have local caches. As with the medium Security Management system, the master configuration database is held in a central control room on a master file server.

Each location will also have a local file server. The local file servers are all synchronised with the central master database either according to a managed schedule (e.g. once a night) or on-demand whenever an administrator makes a change to the site configuration.

At each location, individual workstations talk only to their local file server, never to the master server in the central control room. In addition, each workstation maintains a local cache of the configuration data.

Also, each location has sufficient local storage in the form of NVRs to record all the locally produced video and alarm data.

The advantages of this approach are:

- **Cost:** Managed synchronisation of *static* configuration data across the network means data is only sent on the few occasions there is a change. Even then it can be scheduled to avoid peak bandwidth times. Distributed storage for *live* recording and alarm data means the overall WAN bandwidth required is much lower.
- **Reliability and Resilience:** When the master server fails or the WAN link breaks, operators always have local caches of the Site Database so they can still access any devices on their LAN. In addition, by distributing the recording capability, operators local to an incident will always have access to live video, recorded video and alarm data for their local cameras, even if communication with the central office is down.
- **Scalability:** The Security Management network for a “small” system can be treated as a template for cutting and pasting as many times as necessary. The majority of live data is held locally wherever it is produced and needed. Overall control of the system through site configuration data can still be managed centrally but then distributed in a manner that makes efficient use of wide area networks.

The result is a scalable solution leading to unlimited Security Management system sizes potentially spanning cities, countries and continents.